RECEIVED
CENTRAL FAX CENTER
OCT 19 2007

AMENDMENTS TO THE SPECIFICATION

Please delete the section entitled "SUMMARY OF THE INVENTION" in its entirety and substitute the following section therefor:

SUMMARY OF THE INVENTION

[0021] The present invention, among other applications, is directed to solving these and other problems and disadvantages of the prior art. The present invention provides a superior technique for performing cryptographic operations within a microprocessor. In one embodiment, an apparatus is provided for performing cryptographic operations. The apparatus includes ~~a cryptographic instruction~~fetch logic, keygen logic, and execution logic. The ~~cryptographic instruction is received~~fetch logic receives a cryptographic instruction ~~by a microprocessor~~ as part of an instruction flow executing on the microprocessor. The cryptographic instruction prescribes one of the cryptographic operations, and also prescribes that a provided cryptographic key be expanded into a corresponding key schedule for employment during execution of the one of the cryptographic operations. The keygen logic is disposed within the microprocessor and is operatively coupled to the cryptographic instruction. The keygen logic directs the microprocessor to expand the provided cryptographic key into the corresponding key schedule. The execution logic disposed within the microprocessor and is coupled to the keygen logic. The execution logic expands the provided cryptographic key into the corresponding key schedule.

[0022] One aspect of the present invention contemplates an apparatus for performing cryptographic operations. The apparatus has a cryptography unit within a microprocessor and keygen logic. The cryptography unit executes one of the cryptographic operations responsive to receipt of a cryptographic instruction by the microprocessor within an instruction flow that prescribes the one of the cryptographic operations, where the cryptographic instruction is fetched from memory by fetch logic in the microprocessor, and where the cryptographic instruction also prescribes that a cryptographic key be expanded into a corresponding key schedule be employed when executing the one of the cryptographic operations. The keygen logic is operatively coupled to the cryptography

unit. The keygen logic directs the microprocessor to perform the one of the cryptographic operations and to expand the cryptographic key into the corresponding key schedule.

[0023] Another aspect of the present invention provides a method for performing cryptographic operations. The method includes, within a microprocessor, receiving fetching a cryptographic instruction from memory that prescribes expansion of a cryptographic key into a corresponding key schedule for employment during execution of one of a plurality of cryptographic operations; and within the microprocessor, executing the cryptographic instruction and expanding the cryptographic key into the corresponding key schedule.